ANALYSING ATTACK METHOD WHICH FILE ARE HIGHLY ATTACKED IN CLOUD

[1]Mrs. K. MAHALAKSHMI, [2]M.JEEVANANDHINI
[1]Assistant Professor ,[2]UG Research Scholar
[1]Department of B. Com (Business Analytics)

PSGR Krishnammal College for Women, Coimbatore, Tamilnadu, India,

Abstract Cloud computing provides many advantages, such as speed and efficiency via dynamic scaling. But there are also a host of potential threats in cloud computing This study has been undertaken to analyze using attack method files are highly attack in cloud data. Analyzing the data in cloud and finding the secured, on-secured files,Encrypted and non-encrypted files and to show that the cloud computing is safe or un-safe for users. The objective of this paper is to find the file which is attacked based on cloud and to analyze whether it is attacked in high or low. Analyzing and visualizing the data and finding the results which are made through Random forest algorithm used for data classification Pricing Theory model.

***Key Words*- Analyzing the cloud data, Random forest algorithm, File Attack method.**

I. INTRODUCTION

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software Present, many of the organizations uses cloud computing to share the confidential data. Many hackers trying to violate the security to use the cloud resources.

To keep data secure, the front line of defense for any cloud system is encryption. Encryption methods utilize complex algorithms to conceal cloud-protected information. To decipher encrypted files, would-be hackers would need the encryption key. Although encrypted information is not 100% untraceable, decryption requires a huge amount of computer processing power, forensic software, and a lot of time.

Data in the cloud environment needs to be encrypted at all stages of its transfer and storage:

- at the source (on the user's side)
- in transit (during its transfer from the user to the cloud server)
- at rest (when stored in the cloud database)[1].

Security attack is an intelligent act that attempts to violate the services in the cloud. Different types of attacks are used by the hackers to prevent the cloud users to access the data in the cloud. By working with cloud server uses virtual platform ESX and a VPN network that links to the client. By simulating different scenarios using the Computer Algebra System Magma tools [2].in this paper define which attack methods are highly attacked and which is low attacked file.

II. OBJECTIVE

Analyze using file attack method in cloud data set .which attack method is highly attacked. Analyze the Privacy preserving in cloud environments includes two aspects: data processing security and data storage security. Data processing security covers the issues of how to protect user privacy at runtime in a virtualized cloud platform. Cloud computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability [3]

III. RELATED WORK

While the storage of corporate data on remote servers is not a new development, current expansion of cloud computing justifies a more careful look at its actual consequences involving privacy and confidentiality issues .We introduce in this paper a secure privacy preserving cloud database storage architecture. We focus on the Soft- ware as a Service [4].

Describe a technique through usage of a tamper-proof hardware token. This technique applies to a cloud service provider which is based on trusted computing platform. Another project is from Pearson et al. [5]

The syntax makes embedding of encryption within XML files possible. The XML-encryption includes the following features: encryption of a whole XML document, encryption of a single element and the content of an element. Furthermore, encryption upon encryption is also possible. Geuer-Pollmann [6].

Though many solutions have been proposed earlier many of them only consider one side of security. This component retrieves the data required by the user from the cloud database and thus presents it to the user on the client machine, the cloud data security must be considered to analyse the data security requirements, deployment of security functions, data security process through encryption. The requests are made to access the data from the cloud server through the client machine [7].

Cloud computing is an internet based ubiquitous, on demand network model for convenient network access for pool of configurable computing resources as on demand basis. The software & data that is accessed by the user or a customer may be stored in different servers at different geographical places. This is a security challenge for both the service providers and users.[8].

Cloud service provider for cloud makes sure that the customer is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. Using cloud services or going there, but facing problems with security, privacy and data theft. This makes cloud protection a must to crack the cloud environment's adoption hindrance. Using or switching to cloud services, but facing problems with security, privacy, and data theft. This makes cloud protection a must to crack the cloud environment's acceptance barrier. [9].

The increasing volume of private and sensitive data being harvested by data controllers makes it increasingly necessary to use the cloud not just to store the info, but also to process them on cloud premises. However, security concerns on frequent data breaches, alongside recently upgraded legal data protection requirements (like the ecru Union's General Data Protection Regulation), advise against outsourcing unprotected sensitive data to public clouds. To tackle this issue, this survey covers technologies that allow privacy-aware outsourcing of storage and processing of sensitive data to public clouds [10]

IV. METHODOLOGY

the objectives define Methodology is the specific procedures or techniques used to identify select, process, and analyze information about a topic analysis of the principles of methods, rules, and postulates employed by a discipline systematic study of methods that are, can be, or have been applied within a discipline "the study or description of methods". find whether the files are come under file attack method verified and to show it is high or low the users to use the cloud computing. In this project Random Forest Algorithm is used to find the result .

4. 1 Random Forest Algorithm

Random forest is a supervised learning algorithm. The "forest" it builds, is an ensemble of decision trees, usually trained with the “bagging” method. The general idea of the bagging method is that a combination of learning models increases the overall result **Put simply: random forest builds multiple decision trees and merges them together to get a more accurate and stable prediction.** Random forest has nearly the same hyper parameters as a decision tree or a bagging classifier. Fortunately, there's no need to combine a decision tree with a bagging classifier because you can easily use the classifier-class of random forest.

Random Forest Algorithm works by completing the following steps

Step 1: select file attack method from the dataset.
Step 2: create a decision tree for each sample
Step 3: get a prediction result from each decision tree.
Step 4: perform voting for every predicted result. Use **mod e** for classification problem, and **mean** for a regression.
Step 5: select most voted prediction or final prediction.

The above algorithm performing five major steps to finalize the vote prediction. Here, step 1 selecting the samples from the dataset and step2 created decision tree for each decision samples, step3 getting the decision tree predictions to perform voting with classification algorithm assigns **mode** and **mean** for classification and regression for step4. Finally step5 selects most voted prediction.

IV. RESULTS AND DISCUSSION

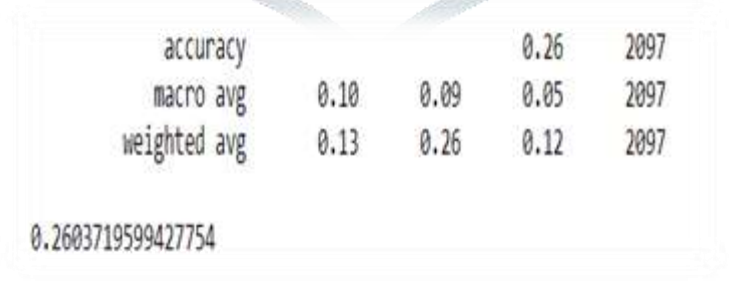

Fig5.1 predicted value

The Above fig5.1 Diagram Represents The file attack method ,Which Is Secured Or Not Secured And Which Is Highly Attacked And Less Attacked .The Above Explains The Train Split Function In Order To Make The Split And Giving The Values To The Variables For X_Train And Y_Train (Prediction Variable And file attack) And Fitting The Model On The Training Data And Trying To Predict The Attributes. To Find The File Which Is Attacked Based On Cloud Name And To Analyze Whether It Is Attacked In Public, Private Or Hybrid. It Predicted The Values Of The Accuracy Score 0.26,Macro Average0.05 And Weighted Average0.12 As Same I.E.,2097, And Matplotlib Is Imported Pyplot In Order To Plot Graphs Of The Data. Finally total value is 0.2603719599427754.

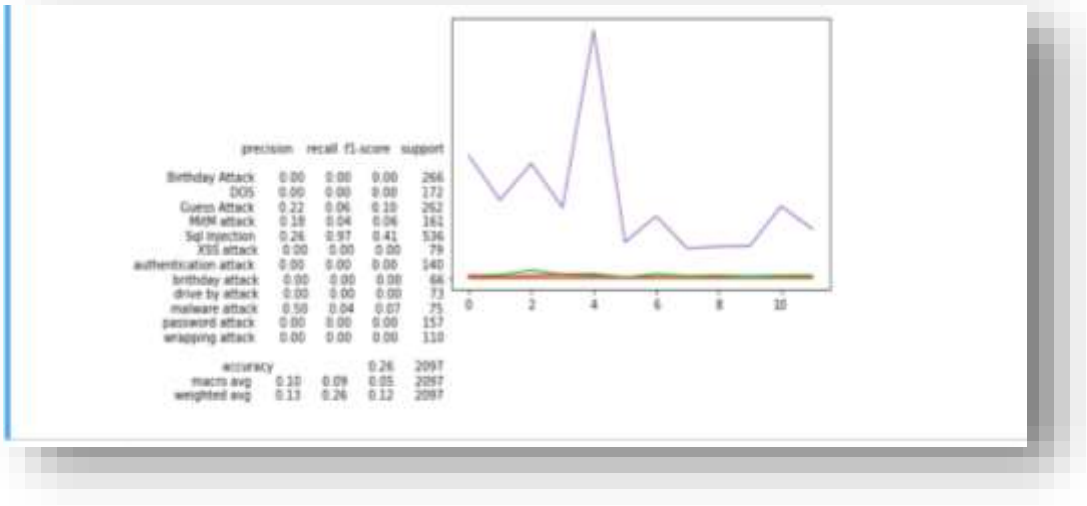

Fig5.2 file attacks

The above fig5.2 diagram represents the file attack method, which is secured or not secured and which is highly attacked and less attacked birthday, doc, guess, Mite, SQL, XSS ,drive ,malware, password ,wrapping are the cloud attack in this by using the Random Forest Classifier Algorithm , to find the files that is highly secured and less attacked. . And it shows the result that is there is more number of encrypted files than a non-encrypted file. So it states that the more files are affected under public cloud computing.

VI. CONCLUSION

The main aim of this paper is to find the attacked files in cloud. predicting which files are secured and non secured , which is affected and not affected ,it is done by using Random Forest Classifier Algorithm .External threats including hacking or other data breaches, whereas internal threats include human error, data loss can be solved by providing security to the cloud. Here the accuracy, macro average, weighted average of value are predicted. Its helps whichever is more attracted by using the Random Forest Classifier Algorithm ,it is easy to predict the result of the files that are uploaded securely to the cloud. Providing data security helps the user or client to secure their information of their data.

References

[1] **Cloud Attack Vectors and Counter Measures – GlobalDots** https://www.globaldots.com › blog › cloud-attack-vectors.
[2] WiebBosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. J. Symbolic Comput., 24(3-4): 235-265, 1997. Computational algebra and number theory, London, 1993.
[3] Qian Wang and Cong Wang and Kui Ren, Wenjing Lou, Jin Li "Enabling Public Auditability And Data Dynamics For Storage Security in Cloud Computing" in IEEE transactions on parallel and distributed systems, 2011, vol. 22, no. 5.
[4] Mowbray, S. Pearson, and Y. Shen, "Enhancing privacy in cloud computing viapolicy-based obfuscation." Springer Berlin/Heidelberg,2010,pp.1–25.
[5]. Ravi Kant Sahu and Abhishek Mohta, L.K. Awasthi "Robust Data Integration While Using Third Party Auditor For Cloud Data Storage Services", conf. IJARCSSE, 2012, Volume 2, Issue 2,ISSN: 2277 128X.
[6].C. Geuer-Pollmann, "Xml pool encryption," in Proceedings of the 2002 ACM workshop on XML security. New York, NY, USA: ACM, 2002, pp. 1–9.
[7] .Merlin Shirly T & Margret Johnson, Improved Security measures for data in key exchanges in Cloud Environment´ in International Journal of research in Computer Applications and Robotics Vol 2 Issue 3, Pg 153- 158, March 2014.
[8]Alena Mehela, (efficient Cryptograptic Techniques for Security Storage System ´ in Thesis submitted for degree of Philretrieve.
[9]. Syam Kumar, P., Subramanian, R., & Thamizh Selvam, D. (2010, 28-30 Oct. 2010). Ensuring (PDGC), 2010 1st International Conference on information corresponding to the label will Be retrieved.
[10]Ali Gholami, "Security and Privacy of Sensitive Data in Cloud Computing", Doctoral Thesis Stockholm, Sweden 2016.